























































































ICANN - easy to censor + fail site

- Not private (usually not encrypted)
- Can be slow (resolving + updating)
- Does not have explicit cache invalidation

How to get from here to there:

- Namespace can be imported - even w/ DNSSEC (key comp)
- Scalability?
- DNSSEC proofs (NSEC3?)
- Name space creation
 - Incentives

Why to do this?

- Censorship
- DNS + PKI
- Programmability / Permissionless innovation

Challenges

Centralization / 91% attacks
names
Flexible









HOW TO...

ICANN - easy to ^{change} + falsify records

- Not private (usually not encrypted) — not unique
- Can be slow (resolving + plotting)
- Does not have explicit cache invalidation

How to get from here to there:

- Name space can be imported - even w/ DNSSEC!
- Scalability → the pricing → market not ^{real} (key complexity)
- DNSSEC proofs (NSEC3)

Name space creation

Secure?

Why to do this?

Censorship

DNS + PKI

• Programmable / Permissionless

What is ICANN's role?

• Short experimental T

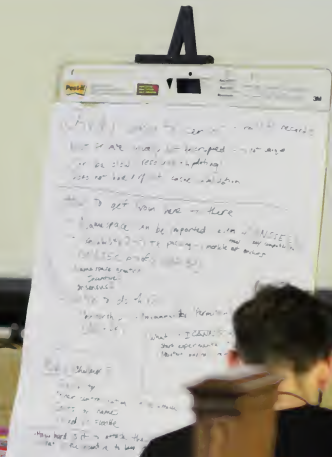
• Monitor barrier to entry

Risks / Challenges

- Scalability
- Minor centralization / 51% attack
- Costs of names
- Fixed vs. Flexible

• Hard to attack the

• What is the incentive to keep



Apply

records are not described - not any
or be slow record updating
not too hard if it's some validation

How to get from here to there

- large page can be imported with NICE
- generate 2-3 page - more or less
- generate 2-3 page - more or less

generate 2-3 page - more or less

generate 2-3 page - more or less

generate 2-3 page - more or less

generate 2-3 page - more or less

generate 2-3 page - more or less

generate 2-3 page - more or less

generate 2-3 page - more or less

generate 2-3 page - more or less

generate 2-3 page - more or less

generate 2-3 page - more or less



RAMN - easier to censor - no history records

- Not private (usually not encrypted) → not unique
- Can be slow (resolving + updating)
- Does not have explicit cache invalidation

How to get from here to there

- Namespace can be imported - even w/ DNSSEC
- Scalability → tx packing → merkle tree
- DNSSEC proofs (NSEC3)
- Namespace creation
 - Transitive? irreversible?
- Why to do this?

Censorship
DNS + PKI

- Programmable / Permissionless
- What is E-CASH?
 - Smart experiments
 - Auction systems

Pro's Challenge 5

- Scalability
- Minor centralization
- Costs of names
- Fixed vs flexible

- How hard is it to attack it?
- What is the incentive to censor?





























